PROCEDURE: No.2205.02 Computer User Responsibilities Procedure
REF: POLICY NO. 2205
EFFECTIVE: 12/28/04
PRIOR ISSUE: 07/31/98

Purpose:

The Arizona Department of Juvenile Corrections establishes standardized procedures to maintain the integrity of the Local Area Network (LAN)/Wide Area Network (WAN) systems, software, hardware, and data. Inappropriate use exposes the Department to risks including virus attacks, compromise of network systems and services, and legal issues.

Rules:

1. All hardware, software, and data are State property and Agency resources. Any use of these resources other than that authorized by ADJC is prohibited. **MIS** will create and provide ADJC staff access rights to appropriate sub-directories that are approved by Employees Supervisor. **AGENCY PERSONNEL** shall follow the guidelines of Procedures 2205.06 and 2205.07 to obtain access to the Internet Browser, GroupWise Messenger, Internet Email, and Web E-mail.

2. **MIS** shall provide all agency personnel with a login and password:
   a. **NETWORK ADMINISTRATORS** shall keep passwords secure and shall not share accounts;
   b. The **USERS** shall choose their personal password which shall be at least 5 alphanumeric characters;
   c. The **USER** shall change the password as needed or every 60 days. After 60 days 5 grace logins will be allowed, after the 5 grace logins have been used, the account shall be locked;
   d. The **USER** is to immediately report it to his/her Supervisor or MIS, if the user's password is compromised at any time;
   e. **USERS** shall not share their passwords amongst agency personnel or family members (for remote access) for individual login accounts;
   f. **USERS** may provide their passwords to MIS when assistance is needed in providing Technical Support;
   g. The **USER** should contact MIS to establish a new password if the user forgets his/her password.

3. **USERS** shall be responsive to all broadcasts and notifications regarding system maintenance. **USERS** shall sign off their workstations prior to the end of their respective work day.

4. Each **FIRST LINE SUPERVISOR** shall notify MIS within 24 hours of an employee's departure from ADJC service so the departed employee's account can be disabled.

5. **ADJC EMPLOYEES** shall not dismantle, disconnect or reconnect, exchange, or physically alter in any manner the location of computer equipment, or the software resident upon it, without the authorization of MIS.

6. **ADJC EMPLOYEES** shall immediately report any physical damage of computer equipment to MIS.

7. **USERS** shall not add privately-owned software and/or hardware to the Department's Local Area Network System (LAN) or the Wide Area Network System (WAN) without receiving prior written approval from the ADJC MIS Administrator.

8. The **USER** shall remove any equipment and/or software supplied by the Department for use on a privately-owned PC from the computer and returned to MIS prior to the user leaving the Department.

9. While ADJC's network administration desires to provide a reasonable level of privacy, **USERS** should be aware that the data they create on state owned systems remains the property of ADJC. Because of the need to protect ADJC's network, management cannot guarantee the confidentiality of information stored on any device belonging to ADJC.

10. For security and network maintenance purposes, **AUTHORIZED INDIVIDUALS WITHIN ADJC** may monitor equipment, systems and network traffic at any time.
    a. **MIS** reserves the right to audit networks and systems on a periodic basis to ensure compliance policy and procedures at any time.

11. **Security and Proprietary Information**
    a. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. **EMPLOYEES** should take all necessary steps to prevent unauthorized access to this information;
    b. **MIS** shall secure all network devices with a password with a timeout feature of inactivity to either log out automatically or ask the user to re-authenticate.
    c. **USERS** shall use encryption of information in compliance with MIS's Acceptable Encryption Use Procedure 2205.04;
    d. **USERS** shall include in ADJC approved postings from an ADJC email address to newsgroups a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ADJC, unless posting is in the course of business duties;
    e. **MIS** shall ensure that all systems used by the employee that are connected to the ADJC Internet/Intranet/Extranet, whether owned by the employee or ADJC, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.

12. **Archiving Records: MIS** shall ensure that any Information Technology (IT) devices (servers, storage, clients), network components, operating system or application software, or storage media containing public/official records have a final disposition of those records established with Department of Library, Archives, and Public Records (DLAPR) before being disposed of through Arizona Department of Administration, Management Services Division, Surplus Property Management Office (SPMO) or provided to another State organization for "reuse."
    a. Clearing Data: Before a storage device is disposed of through SPMO, MIS shall delete data stored on the device in a manner that renders it unrecoverable;
    b. Removal of Sensitive Data: Prior to the disposal, repair and/or scheduled maintenance of an IT device (server, storage, or client), network components, operating system or application software, and storage, or "reuse" by another agency, or for "reuse" by another system within the same agency, **MIS** shall remove all sensitive data from the IT devices (servers, storage, clients), network components, operating system or application software, and storage media. Similarly, the **OWNER**, as defined by the agency, should remove all sensitive data from the IT device (server, storage, and client), network components, operating system or application software, or storage media prior to its disposal;
    c. On storage devices that will be reused, **MIS** may use overwriting or degaussing to replace meaningful data with meaningless data in such a way that the meaningful data cannot be recovered.

13. **Unacceptable Use.** The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration personnel may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an **EMPLOYEE OF ADJC** authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing agency owned resources. Violations of this procedure will result in disciplinary action in accordance with the Agency's Employee Conduct, Procedure 2003.04. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:
    a. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated", or "warez" or other software products that are not appropriately licensed for use by ADJC;

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ADJC or the end user does not have an active license is strictly prohibited;
c. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. MIS should be consulted prior to export of any material that is in question;
d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
e. Using an agency computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;
f. Making fraudulent offers of products, items, or services originating from any ADJC account;
g. Making statements about warranty, expressly or implied, unless it is a part of normal job duties;
h. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
i. Port scanning or security scanning unless prior notification to MIS is made;
j. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty;
k. Circumventing user authentication or security of any host, network or account;
l. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack);
m. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet;
n. Providing information about, or lists of, agency employees to parties outside ADJC. Disclosing ADJC data to anyone outside or within the Department who has not been specifically authorized to receive such data;
o. Archiving or saving printed ADJC data not specifically related to their mandated job duties;
p. Entering, altering, erasing ADJC data outside of authorized job duties;
q. Entering, altering, or erasing ADJC data maliciously, or in response to real or imagined abuse, or for personal amusement;
r. Using ADJC computer hardware for other than work-related purposes;
s. Using software on the Department's local area network (LAN), wide area network (WAN), or on any computer in any manner contrary to the license agreement;
t. Making, acquiring, or using unauthorized copies of computer software;
u. Bringing in software from outside the agency for use on the LAN or individual computer without prior written approval from their supervisor and the MIS Administrator;
v. Loading any department software onto an employee-owned computer without the written approval of the MIS Administrator prior to installation;
w. Failing to disclose any misuse of software or ADJC data/information within the Department;
x. Failing to disclose any personal misuse of software or ADJC data/information as required.

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By: